REMARKS

Claims 1, 18-21, 72-84, and 109-131 are pending in this patent application. Reconsideration of the rejections in view of the remarks below is requested.

The Office Action rejected claims 1, 21, 72, 73, 77, 78, 116-120, 129 and 130 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,745,574 ("Muftic"). Applicant respectfully traverses the rejection, without prejudice.

In disagreeing with Applicant's arguments, the Examiner essentially submits that verifying the authenticity of a request for a certificate of a public key in Muftic amounts to denying access to the public key, i.e., "only those that can create a authentic request have the public key for use" but then finds persuasive that "denying access to a certification authority's public key and in response to a digital signing by the recipient permits a recipient to utilize the public [key]" should be given patentable weight. Respectfully, Applicant submits that is tantamount to saying the claims are patentable and so Applicant can't understand how this action is final and the claims are not allowable.

Even assuming *arguendo* that Muftic discloses denying access to the public key of the certification authority (which Applicant disagrees with as discussed further below), the Examiner appears to agree with Applicant that the remainder of, for example, claim 1 should be given patentable weight but provides no specific argument regarding how that aspect is taught, disclosed or suggested by Muftic. In the absence of teaching, disclosure or suggestion regarding the remainder of claim 1, claim 1 should therefore be allowable. Even if one aspect of a claim is old doesn't mean that the claim as whole is necessarily unpatentable. Rather, as long as one aspect of a claim is new and non-obvious or the combination of aspects in a claim is new and non-obvious, then the claim is patentable. Therefore, since the Examiner admits at least part of claim 1 is patentable or at least provides no specific argument as to how that part is unpatentable in view of Muftic or other prior art, claim 1 is therefore allowable.

Indeed, Applicant submits that the cited portions of Muftic fail to disclose, teach or suggest, *inter alia,* denying access to a certification authority's public key, providing a recipient with at least one message containing rules including a rule regarding maintaining secrecy of said public key, digitally signing said at least one message, by which said recipient agrees to rules, and in response to a digital signing, permitting the recipient to utilize said public key as recited in claim 1. Similarly, Muftic fails to disclose, teach or suggest, *inter alia,* denying use of a public key, providing a recipient with a message containing rules of

said cryptographic system, said rules including a rule regarding maintaining secrecy of said public key; and in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key as recited in claim 73.

For example, the cited portions of Muftic fail to provide any disclosure, teaching or suggestion regarding a message containing a rule regarding maintaining secrecy of a public key as claimed in claims 1 and 73. The Examiner refers to col. 10, lines 52-57 of Muftic but Applicant cannot find anything in that passage about a message containing a rule about secrecy, let alone a rule regarding secrecy of a public key. Rather, there is no indication in the cited portions of Muftic at all that a public key is secret or to be kept secret; in fact, it is the opposite ("In a public key encryption system each participant has two related keys. A public key which is publicly available and a related private key or secret key which is not." Muftic, col. 1, lines 34-36).

Further, for example, the cited portions of Muftic fail to disclose, teach or suggest digitally signing at least one message, by which the recipient agrees to rules as recited in claim 1 and in response to said digital signing, permitting a recipient to utilize said public key as recited in claims 1 and 73. The Examiner refers to col. 11, lines 29-53 and col. 12, lines 32-40 of Muftic but Applicant cannot find anything in those passages about digitally signing a message by which the recipient agrees to rules or in response to such signing permitting a recipient to utilize a public key.

Referring first to the passage in col. 11, lines 29-53, Muftic therein discloses a message sent by an entity to a certifying authority requesting that a public key, enclosed in the message, be certified as authentic (i.e., the applicable public key actually belongs to the entity it is asserted to belong). The certifying authority then checks the public key and if the public key is authentic, returns a signed certificate to the entity to that effect. There is simply nothing there about digitally signing a message by which a recipient agrees to rules – indeed, there is no discussion about rules. Moreover, there is simply nothing in that passage about, in response to such signing, permitting a recipient to utilize a public key. The entity and certifying authority in that passage of Muftic can make use of the public key at any time – the process described there merely addresses whether the public key is authentic, not whether the public key can be used. Denial or affirmance of the authenticity of the public key by the certifying authority does not effect a permission to the entity to utilize a public key but rather denial merely warns the entity that use of the public key may involve risk that the public key

does not belong to who it is asserted to belong (and affirmance signals the opposite).

Further, the passage in col. 12, lines 32-40 of Muftic is merely about establishing the authenticity of a public key by using a chain of certifying authorities, i.e., a series of certificates can be verified so that one party can establish the authenticity of the public key of another party where the two parties, for example, do not share the same certifying authority. There is simply nothing in that passage about digitally signing a message by which the recipient agrees to rules. Moreover, there is nothing about, in response to such signing, permitting a recipient to utilize a public key. The entity and certifying authorities in that passage of Muftic can make use of a public key at any time – that passage is merely about establishing authenticity of a public key.

Finally, Applicant submits that the cited portions of Muftic fail to disclose, teach or suggest denying access to a certification authority's public key as recited in claim 1 and denying use of a public key as recited in claim 73.

The Examiner argues that "Muftic discloses verifying the identity of the entity to which the certificate is being provided in sections column 10 lines 34-49 and further in column 6 lines 47-64 and Fig. 11 with its corresponding description wherein during the process of certification the request for the certificated [sic] is verified for authenticity. The concept of verifying the authenticity of the request is by definition denying access to the public key for the request that is not authentic for use by the processor that the [sic] creates the request that is not authentic" Applicant respectfully disagrees.

A determination by a certifying authority of whether a public key is authentic or not is merely a determination of risk associated with the public key. A certificate is merely an instrument to provide trust regarding the public key (or any other key). Neither issuance or denial of a certificate for a public key affects whether or not the applicable public key can be used or accessed; the issuance or denial of a certificate merely indicates to the requester of the certificate that the public key can be used or accessed with relatively low risk (where a certificate is issued) or with high risk (where a certificate is denied). The certificate can't deny an entity from using or accessing a public key which, in the case of Muftic, the certificate requesting entity and the certifying authority already can use and have access to.

For example, in the cited portions of Muftic, the certificate requesting entity supplies a public key in its possession to the certifying authority for certification and the certifying authority then uses that public key to determine its authenticity. Further, the certificate requesting entity then uses the certifying authority's public key to decrypt the signature of the

certificate supplied by the certifying authority. Thus, the various public keys referred to in the cited portions of Muftic are freely available for access and use by the various entities involved. What the cited portions of Muftic merely address is whether one or more of those public keys are authentic (i.e., the owner of the public key is as purported to be) and if so, confirming or not such to an entity. Thus, the system in Muftic simply aims to identify (and hopefully prevent) tampering (in the sense of modification) of a public key through the use of a conventional signed certificate. However, in no way does the system in Muftic deny access to or use of a public key.

Further, the cite to col. 4, lines 65-67 to col. 5, lines 1-2 in Muftic is inapposite. Muftic merely talks about secure distribution of keys and preventing tampering of keys. This does not provide any disclosure, teaching or suggestion about denying access to or use of a public key. Rather, Muftic indicates that keys are being given to other parties, not denied. At most, Muftic merely indicate that if keys are being distributed they should be done so securely.

Therefore, for at least the above reasons, the cited portions of Muftic fail to disclose, teach or suggest all the features recited by claims 1 and 73. Claims 21, 72, and 116-120 depend from claim 1 and are thus patentable at least for the same reasons as claim 1 and for the additional features recited therein. Claims 77, 78, 129 and 130 depend from claim 73 and are thus patentable at least for the same reasons as claim 73 and for the additional features recited therein As a result, Applicant respectfully maintains that the rejection under 35 U.S.C. §102(e) of claims 1, 21, 72, 73, 77, 78, 116-120, 129 and 130 based on Muftic should be withdrawn and the claims allowed.

Further, the Office Action rejected claims 18, 20, 74, 79, 80, 83, 84, 92, 93, 109-115, 121-125, 127, 128 and 131 under 35 U.S.C. §103(a) as being obvious in view of Muftic and further in view of U.S. Patent No. 5,940,510 ("Curry et al."). Applicant respectfully traverses the rejection, without prejudice. Applicant respectfully submits that the cited portions of Muftic and/or Curry et al. fail to disclose, teach or suggest all the features recited by claims 18, 20, 74, 79, 80, 83, 84, 92, 93, 109-115, 121-125, 127, 128 and 131.

Applicant notes that claims 92 and 93 were previously cancelled by the Amendment filed February 17, 2006. Thus, their rejection is moot.

Claims 18, 20 and 121 depend from claim 1 and claims 74, 122-125, 127, 128 and 131 depend from claim 73. Thus, these claims are patentable over Muftic alone for at least

the same reasons as provided above in respect of claims 1 and 73 respectively above and for the additional features recited therein.

Claim 79 is patentable over Muftic alone at least because the cited portions of Muftic fail to disclose, teach or suggest a method of enforcing a security policy in a cryptographic system comprising, *inter alia*, providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device, and in response to said recipient digitally signing said message, activating said public key in said secure device. The citations to col. 15. lines 32-43 and col. 12, lines 60-64 of Muftic are inapposite. There Muftic merely discloses a certifying authority re-signing a certificate, which involves a certifying authority generating a new key pair for generating the certificate. It fails to provide any disclosure, teaching or suggesting regarding an inactive public key, let alone about a secure device containing the inactive public key and from which the public key cannot be obtained or about activating the public key. Claims 80, 83, 84 and 109-115 depend from claim 79 and are thus patentable at least for the same reasons as claim 79 and for the additional features recited therein.

Further, claims 18, 20, 74, 79, 80, 83, 84, 92, 93, 109-115, 121-125, 127, 128 and 131 are patentable over Curry et al. alone or in combination with Muftic since the cited portions of Curry et al. do not overcome the shortcomings of Muftic, or vice versa.

Curry et al. disclose a secure device that may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device and is not revealed under almost any circumstance. (Curry et al., col. 4, lines 49-52).

However, claims 18, 20 and 121 are patentable over Curry et al. alone or in combination with Muftic at least because the cited portions of Curry et al., whether alone or in combination with Muftic, fail to disclose, teach or suggest, *inter alia,* denying access to a public key and in response to a digital signing, permitting a recipient to utilize said public key as recited in claim 1 from which claims 18, 20 and 121 depend. Similarly, claims 74, 122-125, 127, 128 and 131 are patentable over Curry et al. alone or in combination with Muftic at least because the cited portions of Curry et al., whether alone or in combination with Muftic, fail to disclose, teach or suggest, *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key as recited in claim 73 from which claims 74, 122-125, 127, 128 and 131 depend. Lastly, claims 79, 80, 83, 84 and 109-115 are patentable over Curry et al. alone or in combination with Muftic at least because the cited portions of Curry et al., whether alone or

in combination with Muftic, fail to disclose, teach or suggest, *inter alia,* providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device, and in response to said recipient digitally signing said message, activating said public key in said secure device as recited in claim 79 from which claims 80, 83, 84 and 109-115 depend.

Therefore, for at least the above reasons, the cited portions of Muftic and/or Curry et al. fail to disclose, teach or suggest all the features recited by claims 18, 20, 74, 79, 80, 83, 84, 92, 93, 109-115, 121-125, 127, 128 and 131. As a result, Applicant respectfully submits that the rejection of claims 18, 20, 74, 79, 80, 83, 84, 92, 93, 109-115, 121-125, 127, 128 and 131 under 35 U.S.C. §103(a) should be withdrawn and the claims allowed.

The Office Action also rejected claim 126 under 35 U.S.C. §103(a) as being obvious in view of Muftic, further in view of Curry et al. and further in view of U.S. Patent No. 4,953,209 to Ryder et al. ("Ryder et al."). Applicant respectfully traverses the rejection, without prejudice. Applicant respectfully submits that the cited portions of Muftic, Curry et al. and/or Ryder et al. fail to disclose, teach or suggest all the features recited by claim 126.

Claim 126 depends from claim 73. Thus, this claim is patentable over Muftic alone for at least the same reasons as provided above in respect of claim 73 and for the additional features recited therein.

Further, claim 126 is patentable over Curry et al. alone or in combination with Muftic since the cited portions of Curry et al. do not overcome the shortcomings of Muftic, or vice versa. Curry et al. merely disclose a secure device that may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device and is not revealed under almost any circumstance. (Curry et al., col. 4, lines 49-52). Thus, claim 126 is patentable over Curry et al. alone or in combination with Muftic at least because the cited portions of Curry et al., whether alone or in combination with Muftic, fail to disclose, teach or suggest, *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key as recited in claim 73 from which claim 126 depends.

Further, claim 126 is patentable over Ryder et al. alone or in combination with Muftic and/or Curry et al. since the cited portions of Ryder et al. do not overcome the shortcomings of Muftic and/or Curry et al., or vice versa. Ryder et al. merely disclose a system for electronically transmitting data objects such as computer programs with a means for verifying

that the computer program was actually received and the terms and conditions of its use accepted by the receiver. (Ryder et al., abstract). Ryder et al. is silent about a public key, let alone permitting an entity to utilize a public key. Thus, claim 126 is patentable over Ryder et al. alone or in combination with Muftic and/or Curry et al. at least because the cited portions of Ryder et al., whether alone or in combination with Muftic and/or Curry et al., fail to disclose, teach or suggest, *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key as recited in claim 73 from which claim 126 depends.

Therefore, for at least the above reasons, the cited portions of Muftic, Curry et al. and/or Ryder fail to disclose, teach or suggest all the features recited by claim 126. As a result, Applicant respectfully submits that the rejection of claim 126 under 35 U.S.C. §103(a) should be withdrawn and the claims allowed.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance. If questions relating to patentability remain, the Examiner is invited to contact the undersigned to discuss them.

Should any fees be due, please charge them to our deposit account no. 03-3975, under our order no. 061047/0264493. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced deposit account.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

Jean-Paul G. Hoffman
Reg. No. 42,663
Tel. No. 703-770-7794
Fax No. 703-770-7901

JGH
P. O. Box 10500
McLean, VA 22102
(703) 770-7900